REMARKS

Claims 26-50 are pending. Applicant is adding claims 30-50, amending claims 26 and 29, and canceling claims 1-8 and 18-25.

The Examiner has rejected claims 1-8 and 18-29 under 35 U.S.C. § 112, second paragraph, as being indefinite. Applicant has replaced claims 1-8 and 18-25 with claims 30-51 and amended claim 26 to address the Examiner's concern.

The Examiner has rejected claims 26-29 under 35 U.S.C. § 102(e) as being anticipated by Wood. The Examiner also rejected now canceled claims 1-8 and 18-25 based on Wood alone or in combination with other teachings. Applicant respectfully traverses these rejections.

Wood describes a single sign-on technique in which once a user has been authenticated (e.g., signed on) at a certain trust level, that user need not again be authenticated when accessing a resource that requires that (or a lower) trust level. Each trust level can have an authentication mechanism that is appropriate for the required level of trust. For example, a medium trust level may require that a user be authenticated using a user name and password, while a high trust level may require that a user be authenticated using a biometric technique (e.g., retinal scanning). In addition, Wood describes that the authentication mechanism to be used for a trust level can vary based on environmental information such as time of request, source of request, and connection speed. Wood also describes that multiple authentication mechanisms can be selected for a trust level with the user selecting one of the authentication mechanisms. If a user is presented with an authentication mechanism that the user or the user's computer system does not support, then the user cannot be authenticated.

All the pending claims recite that an authentication methodology is selected based, in part, on the "authentication abilities" of the client computer system or entity. For example, claim 30 recites "the authentication methodology being selected from multiple

authentication methodologies based on authentication abilities and access rights of the client computer system." By selecting an authentication methodology based on authentication abilities, applicant's technique ensures that a server computer system will only attempt to authenticate a client computer system using authentication methodologies that the client computer system is known to support.

Wood, in contrast, neither teaches nor suggests that an authentication mechanism for a trust level is selected based on the knowledge of which authentication mechanism a user can support. For example, Wood may attempt to authenticate a user to a high trust level using digest authentication even though the user cannot generate the digest required for the authentication. Thus, since Wood does not describe that selection is based on authentication abilities, the pending claims are neither anticipated nor obvious in view of Wood. Moreover, selection based on authentication abilities along with the other elements of the pending claims provide a unique combination of elements that is neither taught nor suggested by any relied upon art.

Based upon the above amendments and remarks, applicant respectfully requests reconsideration of this application and its early allowance.

If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-8548.

Dated:

9/14/05

Respectfully submitted,

By Maurice J Pirio

Maurice J. Pirio
Registration No.: 33,273
(206) 359-8548
(206) 359-9548 (Fax)
Attorney for Applicant